

史上最大加密幣案 幣安遭黑客盜491億

平台：已成功凍結234億 願承擔所有損失

網絡安全

加密貨幣交易平台再度發生重大安全事故，全球最大加密貨幣交易所幣安（Binance）披露遭黑客攻擊，涉及資產估計高達63億美元（約491億港元），相信為歷來最大宗加密貨幣盜竊事件。幣安表示，已聯同其他加密貨幣機構緊急凍結約30億美元（約234億港元）相關資產，並承諾承擔所有黑客攻擊損失。事件涉及多條區塊鏈，亦令市場重新關注大型加密貨幣交易平台的資產安全問題。

大公報記者 麥晉璋

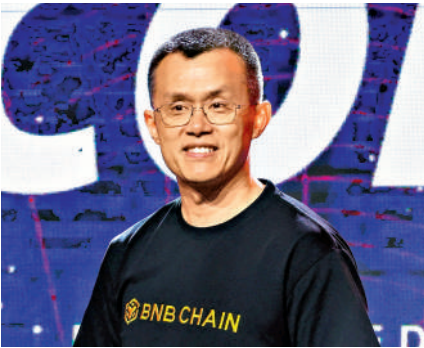
事件發生於周四（29日），幣安發現旗下加密貨幣錢包出現異常資產轉移，隨即展開調查。根據幣安披露的初步結果，黑客可能首先入侵一名負責系統開發及維運的工程師手提電腦，藉此取得內部服務容器（Service Container）的存取權限，並提交未經授權的提款交易。

涉事資產20分鐘內被轉移

美國區塊鏈分析公司TRM Labs公布的調查結果指出，攻擊者從幣安控制的錢包轉移約63.6億美元資產，涉及10條不同區塊鏈，包括以太坊（Ethereum）、比特幣（Bitcoin）、波場（Tron）及Solana等。

根據TRM Labs追蹤的鏈上交易紀錄，大部分資產在約20分鐘內被轉移，顯示攻擊者可能事先已經準備好接收資產的錢包及相關操作程序。由於加密貨幣可以在不同區塊鏈之間轉移，部分資產亦可透過去中心化交易平台進行兌換，因此一旦資金被轉入黑客控制的地址，追查及追回資產將會相當困難。

幣安發現事故後，立即聯絡穩定幣發行商、區塊鏈分析機構及執法部門，嘗試阻止相關資產繼續流轉。平台表示，目前約30億美元受影響資產已被定位及採取凍結措施。其中，全球最大穩定幣USDT發行商Tether表示，已凍結接近15.7億美元相關資產；另一主要穩定幣USDC發行商Circle，則凍結超過8億美元。加密貨幣公司Ripple亦參與行動，涉及約2億美元資產。



▲趙長鵬表示，期望所有用戶獲得全額補償。資料圖片

倘已兌換比特幣 將難以追回

這些資產能夠被凍結，與部分加密貨幣的技術設計有關。以USDT及USDC為例，發行商可以透過智能合約內的黑名單機制，限制指定區塊鏈地址轉移相關代幣。即使黑客已將穩定幣轉入自己的錢包，只要資產仍然屬於可由發行商控制的代幣，發行商便能透過相關機制阻止資產繼續流轉。不過，比特幣及以太幣等原生加密貨幣並沒有相同的中心化發行商凍結機制。因此，若黑客將被盜穩定幣兌換成這類資產，追回資金的難度便會增加。

對於投資者最關注的資產損失問題，幣安聯席行政總裁Richard Teng公開表示，平台將承擔所有黑客攻擊損失，並利用用戶安全資產基金（SAFU）及公司自有資金處理事件。幣安創辦人趙長鵬亦在社交平台表示，期望所有用戶獲得全額補償。此外，幣安昨日更新服務安排，預計48小時內開始逐步恢復提款。

港穩定幣發行商 可依法凍結資產

風險可控

幣安遭黑客攻擊事件，令市場再次關注數碼資產的安全問題。香港近年積極拓展數碼資產市場，滙豐及渣打兩大發鈔銀行的相關機構，亦先後推出受監管的港元穩定幣。由於穩定幣同樣利用區塊鏈技術進行交易，外界關注香港發行的穩定幣會否面臨類似黑客威脅。

對於穩定幣的安全問題，金管局總裁余偉文今年4月發表文章時指出，香港穩定幣監管制度採取「相同活動、相同風險、相同監管」原則，並要求持牌發行商建立全面的風險管理制度，包括儲備資產管理、贖回安排、科技風險及反洗錢措施。這意味著香港持牌穩定幣並非單純依賴發行商自行決定保安標準，而是必須符合監管機構訂立的要求。兩家獲發牌機構亦需要具備相應的風險管理及合規能力，才能開展相關業務。

值得注意的是，香港的穩定幣監管制度亦涉及資產凍結及黑名單機制。根據金管局的反洗錢及反恐融資指引，持

牌發行商須建立風險為本的交易監察制度，利用區塊鏈分析工具識別可疑交易及涉及非法活動的錢包地址，並在適當情況下採取黑名單及凍結措施。

RedCoin存放於私有鏈

例如，當監管機構或執法部門提出符合法律要求的資產凍結要求時，持牌發行商需要具備相應的處理程序。這類機制與Tether及Circle在幣安事件中凍結部分涉案穩定幣的做法，在技術原理上具有相似之處。不過，發行商能否主動凍結特定資產，仍須視乎法律權限、產品條款及實際情況，並非可以在任何情況下任意限制客戶資產。

區塊鏈安全及合規技術公司Beosin於10月發表的研究報告指，RedCoin目前運作於滙豐控制的許可制私有區塊鏈，其技術設計包含黑名單、白名單及緊急控制等功能，有助發行商執行交易管理及合規措施。由於目前使用許可制私有鏈，參與者及交易操作受到一定程度的控制，與一般可自由參與的公開區塊鏈存在分別。

平台安全憂慮升溫 比特幣急挫逾6%

打擊信心

幣安遭黑客攻擊事件迅速衝擊加密貨幣市場。比特幣失守80000美元重要心理關口，一度跌至約76000美元，24小時跌幅超過6%，以太幣及其他主要加密貨幣亦受到沽壓。市場除了關注幣安能否追回被轉移的資產，更擔心事件可能打擊機構投資者對加密貨幣交易平台有信心。

由於幣安是全球交易量最大的加密貨幣交易平台，事故令市場憂慮交易所的資產安全及流動性問題，投資

者紛紛減持相關資產。比特幣在消息傳出後跌穿80000美元，並一度下試76000美元水平，創約6星期低位。

另一個值得留意的現象是槓桿交易令跌勢進一步擴大。CoinDesk引述市場數據指出，昨日加密貨幣期貨市場的強制平倉金額約15億美元，其中比特幣相關倉位約4.68億美元，以太幣約3.58億美元，主要涉及押注價格上升的好倉。

資深加密貨幣炒家Elvis表示，當比特幣急跌，部分使用高槓桿的投資

者因保證金不足而被迫平倉，相關沽盤又可能進一步壓低價格，形成短期連鎖反應。因此，幣安事故雖然並非直接涉及比特幣區塊鏈本身遭到入侵，仍足以透過市場信心及槓桿交易影響幣價。

黑客料難大規模拋售

渣打銀行全球數碼資產研究主管Geoffrey Kendrick表示，幣安疑遭黑客攻擊及相關資產被凍結的消息，已令加密貨幣價格明顯下跌，而且跌

勢將較大機會持續，只有待被凍結資產的處理情況更加明朗，以及更多事故細節公布後，市場才可能重拾信心。

另香港ViaBTC首席分析師Jeff Ko表示，雖然比特幣地址不能由發行商凍結，但每筆鏈上交易均可追蹤，黑客要大規模出售被盜比特幣並不容易，相信這批被盜比特幣不會對市場構成太大的額外沽壓。他更提到，2025年Bybit遭黑客攻擊後，加密貨幣市場只用了數星期便恢復。



▲幣安披露遭黑客攻擊，並轉移高達63億美元的資產，相信是歷來最大宗加密貨幣盜竊事件。資料圖片

網傳幣安遭遇黑客攻擊過程

2026年10月29日（當地時間）

14:00

黑客組織TraderTraitor成功入侵幣安內部一名DevOps高級工程師的個人手提電腦。

14:15

黑客利用該電腦的特權，成功滲透內部服務容器，繞過常規審批，直接取得巨額提款的授權。

14:20

黑客啟動自動化腳本，從幣安熱錢包一口氣捲走高達63億美元資產，並在短時間內將資金分散流向以太坊、比特幣等10條不同的區塊鏈

14:35

幣安資安系統偵測到異常巨額流出，高層緊急下令全面暫停全平台的充值與提現功能，並聯絡各大穩定幣發行商

14:40

黑客利用發行商反應的時間差，在最初20分鐘內，通過去中心化交易所（DEX）將穩定幣兌換成比特幣或以太幣等「無法被凍結」的原生資產，涉資約33億美元；另有約30億美元則已被定位及採取凍結措施

15:00

幣安創辦人公開承諾：用戶資金安全，所有未能追回的損失將由公司「用戶安全資產基金（SAFU）」及自有資金「全額承擔」

大公報記者整理

近期加密貨幣交易平台 重大安全事故

幣安
（今年10月）



事件：黑客入侵幣安員工個人手提電腦，並迅速從熱錢包捲走高達63億美元資產

Bybit
（去年2月）



事件：黑客透過針對前端與開發者工具簽名漏洞攻擊，非法轉移價值約14.6億美元的以太坊資產

Bitget
（今年9月）



事件：黑客利用第三方安全產品的漏洞，向系統發送偽造提現指令和竊取資產，估計損失金額約3.88億美元

大公報記者整理

長揸加密幣 冷錢包較安全

加強保護

隨著加密貨幣市場持續發展，除了普通散戶投資者，家族辦公室及高資產淨值人士亦逐漸增加對數碼資產的關注。然而，幣安遭黑客攻擊事件再次令市場關注資產託管風險。即使選擇規模龐大的交易平台，亦不代表資金完全安全。對於打算中長期持有加密貨幣的投資者，冷錢包（Cold Wallet）是其中一種值得考慮的資產保管方式。

資深加密貨幣炒家Elvis表示，一般加密貨幣交易平台為了處理客戶的即時買賣及提款需求，需要使用熱錢包（Hot Wallet）管理部分資產。熱錢包的私鑰管理或交易簽署環境通常與互聯網連接，方便用戶快速轉移資金，但亦增加受到惡意程式、釣魚攻擊或系統權限被盜用的風險。

轉移需用硬件裝置簽署

冷錢包則採用不同的保管方式，主要透過離線環境保存私鑰，常見形式包括硬件錢包。當投資者需要轉移加密貨幣時，可以利用硬件裝置簽署交易，而

毋須將私鑰直接暴露於連接互聯網的電腦。由於私鑰主要離線保存，黑客較難單純透過遠端網絡攻擊取得相關資料，因此冷錢包較適合不需要頻繁交易、打算長期持有比特幣或以太幣的投資者。

不過，冷錢包並非絕對安全。若投資者遭騙徒誘使透露恢復助記詞（Seed Phrase），或者錯誤授權惡意交易，資產仍可能被盜。若助記詞遺失而又沒有其他恢復方法，亦可能永久失去資產。因此，投資者應妥善保管助記詞，避免將其拍照或儲存在雲端設備，並在轉移大額資產前先進行小額測試。



▲冷錢包內的加密貨幣以硬件裝置簽署交易。法新社

熱冷錢包大比拼

熱錢包 （Hot Wallet）	項目	冷錢包 （Cold Wallet）
私鑰管理或簽署環境通常在線	網絡連接	私鑰主要離線保存
日常交易、轉賬及支付	主要用途	中長期持有及資產保管
方便快捷操作及調動資金	交易便利性	轉賬通常需要額外裝置操作
較容易受到遠端入侵及惡意程式威脅	網絡攻擊風險	可降低私鑰遭遠端盜取的風險
可由用戶自行保管或交由平台託管	私鑰管理	可自行保管或採用專業機構託管
取決於私鑰、賬戶及交易授權系統的保護	資產安全	私鑰離線保存，但仍須防範釣魚及惡意交易
賬戶被盜、平台倒閉或提款受限制	資產遺失風險	助記詞遺失且無法恢復時可能永久失去資產
通常可透過備份或賬戶恢復機制處理	設備遺失	硬件裝置遺失後可使用安全保存的助記詞恢復
軟件錢包通常免費	使用成本	硬件錢包一般需要購買設備
頻繁買賣的短線投資者	適合投資者	不需頻繁交易的中長線投資者

大公報記者整理

趙長鵬回應馬斯克：現在不是嘲諷時候

【大公報訊】一向緊貼市場的SpaceX創辦人馬斯克（Elon Musk），在社群平台X貼上嘲諷表情符號，並「Tag」（標籤）了趙長鵬，以趁機對幣安失竊事件的嘲弄，事件引起趙長鵬的不滿。

趙長鵬帖文：「Elon，我非常尊重你，但現在不是嘲諷的好時候。請停止。」他同時提醒，其持有價值超過10億美元的SpaceX股份，「如果你能給予一點支持，我們將不勝感激。」馬斯克其後再在X上以大笑臉和火焰表情符號作回應。